

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

**Accessing a Server Using a User
Authentication Indicator**

Inventor(s):

John Hal Howard

Jeffrey C. Kunins

Darren L. Anderson

Ryan W. Battle

Max E. Metral

RELATED APPLICATIONS

This application is a continuation of U.S. Application Serial No. 09/350,018 filed July 8, 1999 and entitled "Controlling Access To A Network Server Using An Authentication Ticket", incorporated by reference herein for all that it discloses and teaches.

TECHNICAL FIELD

This invention relates to network access systems. More particularly, the invention relates to the control of access to a network by a user through an authentication server that generates an authentication ticket indicating whether the user has been authenticated.

BACKGROUND OF THE INVENTION

The recent growth in popularity of the Internet has significantly increased the number of Internet users and the number of Internet sites (also referred to as "web sites"). Web sites may provide various types of information to users, offer products or services for sale, and provide games and other forms of entertainment. Many web sites require users to "register" by providing information about themselves before the web server grants access to the site. This registration information may include the user's name, account number, address, telephone number, email address, computer platform, age, gender, or hobbies. The registration information collected by the web site may be necessary to complete transactions (such as commercial or financial transactions). Additionally, information can be collected which allows the web site operator to learn about the visitors to the site to better target its future marketing activities or adjust the

1 information provided on the web site. The collected information may also be used
2 to allow the web site to contact the user directly (e.g., via email) in the future to
3 announce, for example, special promotions, new products, or new features of the
4 web site.

5 When registering with a web site for the first time, the web site typically
6 requests that the user select a login ID and an associated password. The login ID
7 allows the web site to identify the user and retrieve the user's information during
8 subsequent user visits to the web site. Generally, the login ID must be unique to
9 the web site such that no two users have the same login ID. The password
10 associated with the login ID allows the web site to authenticate the user during
11 subsequent visits to the web site. The password also prevents others (who do not
12 know the password) from accessing the web site using the user's login ID. This
13 password protection is particularly important if the web site stores private or
14 confidential information about the user, such as financial information or medical
15 records.

16 If a user visits several different web sites, each web site may require entry
17 of similar registration information about the user, such as the user's name, mailing
18 address, and email address. This repeated entry of identical data is tedious when
19 visiting multiple web sites in a short period of time. Many web sites require the
20 user to register before accessing any information provided on the web site. Thus,
21 the user must enter the requested registration information before they can
22 determine whether the site contains any information of interest.

23 After registering with multiple web sites, the user must remember the
24 specific login ID and password used with each web site or other Internet service.
25 Without the correct login ID and password, the user must re-enter the registration

1 information. A particular user is likely to have different login IDs and associated
2 passwords on different web sites. For example, a user named Bob Smith may
3 select "smith" as his login ID for a particular site. If the site already has a user
4 with a login ID of "smith" or requires a login ID of at least six characters, then the
5 user must select a different login ID. After registering at numerous web sites, Bob
6 Smith may have a collection of different login IDs, such as: smith, smith1,
7 bsmith, smithb, bobsmith, bob_smith, and smithbob. Further, different passwords
8 may be associated with different login IDs due to differing password requirements
9 of the different web sites (e.g., password length requirements or a requirement that
10 each password include at least one numeric character). Thus, Bob Smith must
11 maintain a list of web sites, login IDs, and associated passwords for all sites that
12 he visits regularly.

13 14 **SUMMARY OF THE INVENTION**

15 A mechanism for seeking access of a client to a first server is described.
16 The mechanism involves determining that a client seeking access to the first server
17 is not authenticated by an authentication server. The mechanism further involves
18 communicating a request for login information to be returned to the second server
19 from the client. Login information is received at the authentication server from
20 the client. The client is authenticated by comparing the login information with
21 authentication information maintained by the authentication server. When the
22 login information matches the authentication information, a user authentication
23 indicator (which in one version is an authentication ticket) is generated at the
24 authentication server and the user sends the authentication indicator to the first
25

1 server.

2 An implementation of the invention receives a request from a network
3 server to authenticate a user who is seeking access to the network server. The
4 process determines whether the user was already authenticated by the
5 authentication server. If the user was already authenticated, then the network
6 server is notified that the user is authenticated through the use of a user
7 authentication indicator. If the user was not already authenticated by the
8 authentication server, then login information is retrieved from the user and
9 compared to authentication information maintained by the authentication server.
10 The network server is notified (through the use of the user authentication
11 indicator) that the user is authenticated if the retrieved login information matches
12 the authentication information.

13 Other aspects of the invention provide for the user authentication indicator
14 that does not contain any reference to the user's login information.

15 In accordance with another aspect of the invention, the user authentication
16 indicator includes a first time stamp indicating the last time the user's login
17 information was refreshed, and a second time stamp indicating the last time the
18 user physically entered their login information.

19 In one embodiment of the invention, the network server is a web server
20 coupled to the Internet.

21 22 **BRIEF DESCRIPTION OF THE DRAWINGS**

23 Fig. 1 illustrates an exemplary network environment in which the present
24 invention is utilized.
25

1 Fig. 2 is a block diagram showing pertinent components of a computer in
2 accordance with the invention.

3 Figs. 3 and 4 illustrate the interaction between the client computer system, a
4 particular affiliate server and the authentication server when a user of the client
5 computer system seeks access to the affiliate server.

6 Figs. 5 and 6 illustrate the interaction between the client computer system, a
7 particular affiliate server and the authentication server in a different situation.

8 9 **DETAILED DESCRIPTION**

10 Fig. 1 illustrates an exemplary network environment in which the present
11 invention is utilized. A client computer system 100 is coupled to a network 102.
12 In this example, network 102 is the Internet (or the World-Wide Web). However,
13 the teachings of the present invention can be applied to any data communication
14 network. Multiple affiliate servers 104, 106, and 108 are coupled to network 102,
15 thereby allowing client computer system 100 to access web servers 104, 106, and
16 108 via the network. Affiliate servers 104, 106, and 108 are also referred to as
17 “web servers” and “network servers”. An authentication server 110 is also
18 coupled to network 102, allowing communication between the authentication
19 server and client computer system 100 and web servers 104, 106, and 108.
20 Although referred to as an “authentication server”, authentication server 110 is
21 also a web server capable of interacting with web browsers and other web servers.
22 In this example, data is communicated between the authentication server, client
23 computer system, and web servers using the hypertext transfer protocol (http), a
24 protocol commonly used on the Internet to exchange information.
25

1 An authentication database 112 is coupled to authentication server 110.
2 The authentication database 112 contains information necessary to authenticate
3 users and also identifies which elements of the user profile information should be
4 provided to a particular affiliate server when the user accesses the affiliate server.
5 Although the authentication database 112 is shown separately from the
6 authentication server 110, in other embodiments of the invention, the
7 authentication database is contained within the authentication server.

8 The authentication process, as described below, authenticates a user of
9 client computer 100 seeking access to an affiliate server 104, 106, or 108. The
10 authentication server 110 authenticates the user of client computer 100 by
11 requesting authenticating information, such as the user's login ID and password.
12 If the user is successfully authenticated, then authentication server 110 generates
13 an authentication ticket and communicates the ticket to the appropriate affiliate
14 server. The authentication ticket indicates that the user is authenticated.
15 Additional details regarding the authentication ticket are provided below.

16 As part of the user authentication process, the authentication server 110
17 may provide certain user profile information to the affiliate server, such as the
18 user's email address, user preferences, and the type of Internet browser installed
19 on client computer 100. This user profile information is associated with the user's
20 login ID so that each time the user logs into an affiliate server, the associated user
21 profile information is available to provide to the affiliate server. This user profile
22 allows the user to enter the information once and use that information during
23 subsequent logins to new affiliate servers.

24 The term "affiliate server" is defined herein as a web server that has
25 "registered" or otherwise established a relationship or affiliation with the

1 authentication server 110. Each affiliate server 104, 106, and 108 includes a code
2 sequence (not shown) that allows the affiliate server to communicate with the
3 authentication server 110 when a user (who is also registered with the
4 authentication server) requests access to the affiliate server. Additional details
5 regarding the authentication process and the interaction between the client
6 computer, the affiliate servers, and the authentication server are provided below.

7 Fig. 2 shows a general example of a computer 130 that can be used with the
8 present invention. A computer such as that shown in Fig. 2 can be used for client
9 computer system 100, authentication server 110, or any of the affiliate servers 104,
10 106 or 108.

11 Computer 130 includes one or more processors or processing units 132, a
12 system memory 134, and a bus 136 that couples various system components
13 including the system memory 134 to processors 132. The bus 136 represents one
14 or more of any of several types of bus structures, including a memory bus or
15 memory controller, a peripheral bus, an accelerated graphics port, and a processor
16 or local bus using any of a variety of bus architectures. The system memory 134
17 includes read only memory (ROM) 138 and random access memory (RAM) 140.
18 A basic input/output system (BIOS) 142, containing the basic routines that help to
19 transfer information between elements within computer 130, such as during start-
20 up, is stored in ROM 138.

21 Computer 130 further includes a hard disk drive 144 for reading from and
22 writing to a hard disk (not shown), a magnetic disk drive 146 for reading from and
23 writing to a removable magnetic disk 148, and an optical disk drive 150 for
24 reading from or writing to a removable optical disk 152 such as a CD ROM or
25 other optical media. The hard disk drive 144, magnetic disk drive 146, and optical

1 disk drive 150 are connected to the bus 136 by an SCSI interface 154 or some
2 other appropriate interface. The drives and their associated computer-readable
3 media provide nonvolatile storage of computer-readable instructions, data
4 structures, program modules and other data for computer 130. Although the
5 exemplary environment described herein employs a hard disk, a removable
6 magnetic disk 148 and a removable optical disk 152, it should be appreciated by
7 those skilled in the art that other types of computer-readable media which can
8 store data that is accessible by a computer, such as magnetic cassettes, flash
9 memory cards, digital video disks, random access memories (RAMs), read only
10 memories (ROMs), and the like, may also be used in the exemplary operating
11 environment.

12 A number of program modules may be stored on the hard disk 144,
13 magnetic disk 148, optical disk 152, ROM 138, or RAM 140, including an
14 operating system 158, one or more application programs 160, other program
15 modules 162, and program data 164. A user may enter commands and information
16 into computer 130 through input devices such as a keyboard 166 and a pointing
17 device 168. Other input devices (not shown) may include a microphone, joystick,
18 game pad, satellite dish, scanner, or the like. These and other input devices are
19 connected to the processing unit 132 through an interface 170 that is coupled to
20 the bus 136. A monitor 172 or other type of display device is also connected to the
21 bus 136 via an interface, such as a video adapter 174. In addition to the monitor,
22 personal computers typically include other peripheral output devices (not shown)
23 such as speakers and printers.

24 Computer 130 commonly operates in a networked environment using
25 logical connections to one or more remote computers, such as a remote computer

1 176. The remote computer 176 may be another personal computer, a server, a
2 router, a network PC, a peer device or other common network node, and typically
3 includes many or all of the elements described above relative to computer 130,
4 although only a memory storage device 178 has been illustrated in Fig. 2. The
5 logical connections depicted in Fig. 2 include a local area network (LAN) 180 and
6 a wide area network (WAN) 182. Such networking environments are
7 commonplace in offices, enterprise-wide computer networks, intranets, and the
8 Internet.

9 When used in a LAN networking environment, computer 130 is connected
10 to the local network 180 through a network interface or adapter 184. When used
11 in a WAN networking environment, computer 130 typically includes a modem 186
12 or other means for establishing communications over the wide area network 182,
13 such as the Internet. The modem 186, which may be internal or external, is
14 connected to the bus 136 via a serial port interface 156. In a networked
15 environment, program modules depicted relative to the personal computer 130, or
16 portions thereof, may be stored in the remote memory storage device. It will be
17 appreciated that the network connections shown are exemplary and other means of
18 establishing a communications link between the computers may be used.

19 Generally, the data processors of computer 130 are programmed by means
20 of instructions stored at different times in the various computer-readable storage
21 media of the computer. Programs and operating systems are typically distributed,
22 for example, on floppy disks or CD-ROMs. From there, they are installed or
23 loaded into the secondary memory of a computer. At execution, they are loaded at
24 least partially into the computer's primary electronic memory. The invention
25 described herein includes these and other various types of computer-readable

1 storage media when such media contain instructions or programs for implementing
2 the steps described below in conjunction with a microprocessor or other data
3 processor. The invention also includes the computer itself when programmed
4 according to the methods and techniques described below.

5 For purposes of illustration, programs and other executable program
6 components such as the operating system are illustrated herein as discrete blocks,
7 although it is recognized that such programs and components reside at various
8 times in different storage components of the computer, and are executed by the
9 data processor(s) of the computer.

10 Prior to executing the authentication process described below, both the user
11 of client computer system 100 and the operator of affiliate server 104 "register"
12 with the authentication server 110. This registration is a one-time process which
13 provides necessary information to the authentication server. The user of client
14 computer system 100 registers by providing the user's name, mailing address,
15 email address, and various other information about the user or the client computer
16 system. As part of the user registration process, the user is assigned (or selects) a
17 login ID, which is a common login ID used to access any affiliate server. The
18 login ID may also be referred to herein as a "user name" or "login name".
19 Additionally, the user selects a password associated with the login ID which is
20 used for authentication purposes. After registering and logging into the
21 authentication server, the user can visit any affiliate server (i.e., affiliate servers
22 that are also registered with the same authentication server) without requiring any
23 additional authentication and without re-entering user information that is already
24 contained in the associated user profile.

1 The operator of affiliate server 104 registers with the authentication server
2 110 by providing information about the affiliate server (e.g., server name and
3 internet address). Additionally, the affiliate server provides information regarding
4 its authentication requirements. The authentication requirements can be specified
5 as the maximum time allowed since the last login and entry of authentication
6 information by the user as well as the maximum time allowed since the last
7 “refresh” of the authentication information by the user. Refreshing the
8 authentication information refers to the process of having the user re-enter the
9 password to be certain that the appropriate user is still operating the client
10 computer system. This periodic refreshing of authentication information is useful
11 if the user leaves their computer system without logging out of the authentication
12 server, thereby allowing another individual to access affiliate servers using the
13 login ID of the previous user. If a user requests access to the affiliate server after
14 the maximum time allowed, then the user is re-authenticated (i.e., refreshed) by
15 the authentication server by issuing a new authentication ticket. Thus, although
16 there is a central authentication server, each individual affiliate server can establish
17 its own authentication requirements which are enforced by the authentication
18 server. After registering with the authentication server, the affiliate server can use
19 the authentication server to authenticate any user that has also registered with the
20 authentication server.

21 Figs. 3 and 4 illustrate the interaction between the client computer system
22 100, the affiliate server 104, and the authentication server 110 when a user of the
23 client computer system seeks access to the affiliate server. The example illustrated
24 with respect to Figs. 3 and 4 describes the situation in which the user of the client
25 computer system 100 has not yet logged into the affiliate server 104 and has not

1 yet been authenticated by the authentication server 110. The lines in Fig. 3 labeled
2 “A” through “H” represent the flow of information or activities during the
3 authentication process. The arrows on the lines indicate the direction of the
4 process flow. The label “A” represents the beginning of the process and the label
5 “H” represents the end of the process. The corresponding steps in Fig. 4 are
6 indicated with the label in parenthesis.

7 Fig. 4 is a flow diagram illustrating the authentication process when a user
8 of the client computer system 100 seeks access to the affiliate server 104. The
9 process begins when the user of the client computer system accesses a web page
10 on the affiliate server (step 200). The client computer system includes a web
11 browser, such as the “Internet Explorer” web browser manufactured and
12 distributed by Microsoft Corporation of Redmond, Washington, for accessing
13 various web sites. The affiliate server determines whether the user seeking access
14 to the server is already logged into the affiliate server (e.g., authenticated) at step
15 202. In this example, the user is not logged into the affiliate server, so the user
16 must be authenticated before the affiliate server will allow access. To authenticate
17 the user, the affiliate server redirects the user’s browser to the authentication
18 server.

19 In this example, the user has not yet logged into the authentication server.
20 Thus, the authentication server generates a sign-in web page and communicates
21 the web page to the client computer system for display on the user’s browser (step
22 204). The sign-in web page requests the user’s login ID and password, which
23 were established when the user registered with the authentication server. The user
24 fills-in the requested information on the sign-in web page and clicks a “sign-in”
25

1 button on the web page to send the information entered to the authentication server
2 (step 206).

3 Upon receiving the information from the user of the client computer
4 system, the authentication server compares the entered information with the
5 information stored in the authentication database (step 208). If the user-entered
6 information is not correct (i.e., does not match the information stored in the
7 authentication database) then the authentication server generates and
8 communicates a web page to the user indicating the login ID and password
9 combination were not valid (step 210). The web page may give the user an
10 opportunity to re-enter the login ID and password by returning to step 204.
11 Confidential information (such as the login ID and password) is communicated
12 using a secure protocol such as SSL (secure sockets layer). Various other secure
13 protocols or encryption mechanisms can be used to communicate confidential
14 information between the authentication server and the client computer system.

15 If the user-entered information is correct (i.e., matches the information
16 stored in the authentication database) then the authentication server copies the
17 appropriate cookies to the client computer system and redirects the user's browser
18 to the affiliate server (step 212). A "cookie" is a piece of data provided to a web
19 browser by a web server. The data (i.e., cookie) is sent back to the web server by
20 the web browser during subsequent accesses to the web server. With respect to
21 step 212, one cookie contains information regarding the date and time that the user
22 was authenticated by the authentication server. Another cookie contains
23 information regarding the user profile. The authentication server also updates (or
24 creates) a cookie that contains a list of all sites (or web servers) visited by the user
25 since the last logout from the authentication server. The cookie is updated by

1 adding the current affiliate server to the list of sites visited. This list of sites
2 visited is used to remove cookies from the client computer system when the user
3 logs out of the authentication server. For example, when the user logs out, the
4 authentication server sends a message to each web server on the list of sites
5 visited. Each message is a request for the web server to delete any cookies it
6 placed on the client computer system (e.g., through a browser running on the client
7 computer system).

8 Cookies written to the client computer system by the authentication server
9 cannot be read by any affiliate server. Similarly, cookies written to the client
10 computer system by a particular affiliate server cannot be read by any other
11 affiliate server. The cookies written by an affiliate server are encrypted using a
12 key that is unique to the affiliate server, thereby preventing other affiliate servers
13 from reading the data stored in the cookies.

14 Step 212 also includes generating an authentication ticket and transmitting
15 the ticket to the affiliate server. The authentication ticket is generated by the
16 authentication server and indicates whether a particular user has been
17 authenticated by the authentication server. To protect the user's password and
18 other login information, the affiliate server receives the authentication ticket
19 instead of the user's password and other login information. The authentication
20 ticket indicates that the user is authenticated and how much time has elapsed since
21 the user was last authenticated.

22 The authentication server also communicates the user profile information to
23 the affiliate server (step 214) through the client computer system. In a particular
24 embodiment of the invention, the user of the client computer system can specify
25 during the registration process what types of profile information should be

1 provided to various types of web servers. For example, a user may specify that all
2 commerce-related web servers should receive the user's mailing address, but
3 restrict the mailing address from all other types of web sites.

4 After receiving the authentication ticket and the user's profile information,
5 the affiliate server generates a personalized web page for the user and
6 communicates the web page to the user's browser (step 216). Additionally, the
7 affiliate server copies one or more cookies to the client computer system which
8 include information indicating that the user of the client computer system has been
9 authenticated and indicating the period of time during which the authentication is
10 valid. Each time the user enters a new web page request on the same affiliate
11 server, the data in the cookie is copied to the affiliate server along with the page
12 request. Thus, the affiliate server will not repeatedly check the authentication of a
13 user during each subsequent page request. However, if a particular period of time
14 has passed (referred to as a timeout period) since the last authentication process by
15 the authentication server, then the affiliate server may request a re-authorization of
16 the user.

17 The authentication ticket discussed above contains two time stamps. The
18 first time stamp indicates the last time that the user's login ID and password were
19 physically typed by the user. The second time stamp indicates the last time that
20 the user's login information was refreshed by the authentication server. This
21 "refresh" of the user's login information can be performed "silently" or by manual
22 entry of the login information (i.e., login ID and password) by the user. The
23 refreshing of the user's login information is performed by the authentication
24 server. Once completed, a new authentication ticket is issued to the affiliate server
25 indicating the new time stamp values. If the refresh operation fails (i.e., the user

1 does not supply the correct login information), then the user is logged out of the
2 authentication server and all affiliate servers.

3 Each affiliate server can specify the minimum time requirements for each
4 time stamp in the authentication ticket. If either time stamp exceeds the minimum
5 time requirement for the affiliate server, then the authentication server is contacted
6 to re-authenticate (or refresh) the user login information and update the time
7 stamps accordingly. Each authentication ticket is encrypted using the affiliate
8 server's shared encryption key, thereby preventing other affiliate servers from
9 viewing the authentication ticket.

10 If the user of the client computer system is new to the affiliate server, the
11 affiliate server may request additional user information that is not already
12 contained in the user profile. The additional information may include information
13 unique to that site (e.g., account number) or information about the user's
14 preferences and how the user intends to use the web site. Thus, although the user
15 generates a user profile that is stored on the authentication server, the user may be
16 required, during an initial visit to a web site, to provide additional information for
17 the benefit of the associated web server. This additional information is then stored
18 by the affiliate server such that the user will not be required to re-enter the data
19 during subsequent visits to the same web site.

20 Although affiliate server 104 and authentication server 110 are both
21 coupled to network 102 (see Fig. 1), no direct connections are shown in Fig. 3. In
22 this embodiment of the invention, the affiliate server 104 and the authentication
23 server 110 do not communicate directly with one another. Instead,
24 communications between the affiliate server and the authentication server pass
25 through the client computer system. However, in an alternate embodiment of the

1 invention, affiliate server 104 communicates directly with authentication server
2 110, using network 102 or another data communication medium. Thus, rather
3 than communicating through client computer system 100, the communications
4 flow directly between the authentication server and the affiliate server. Although
5 the authentication server and the affiliate server communicate directly, the user's
6 authentication information (e.g., password) is not exposed to the affiliate server.

7 After a user has logged into the authentication server, it is not necessary to
8 re-enter the login ID, password, or other user information when accessing other
9 affiliated web servers. The subsequent affiliate web servers accessed will
10 determine from the authentication server that the user is already authenticated.

11 Figs. 5 and 6 illustrate the interaction between the client computer system, a
12 particular affiliate server and the authentication server in a different situation. The
13 example illustrated with respect to Figs. 5 and 6 describes the situation in which
14 the client computer system 100 has already been authenticated by the
15 authentication server 110 (e.g., when logging into a different affiliate server), but
16 the client computer system is not yet logged into the affiliate server 104.

17 In this example, the user of the client computer system 100 accesses a web
18 page on the affiliate server 104 (step 230). The affiliate server determines that the
19 user is not authenticated (with respect to the affiliate server) and redirects the
20 user's browser to the authentication server (step 232). Next, the authentication
21 server retrieves the affiliate information entered during registration of the affiliate
22 to determine whether the most recent authentication of the user is within the
23 affiliate's timeout period (step 234). If the most recent authentication is not within
24 the timeout period (i.e., not acceptable), then the authentication server retrieves
25

1 and authenticates the user's login ID and password (step 238) using, for example,
2 the procedures discussed above with respect to Fig. 4.

3 If the most recent authentication is acceptable, then the authentication
4 server copies the appropriate cookies to the client computer system and redirects
5 the user's browser back to the affiliate server (step 240). Additionally, the
6 authentication server generates an authentication ticket, which is communicated to
7 the affiliate server. As discussed above, the authentication ticket indicates to the
8 affiliate server that the user is authenticated. Furthermore, the authentication
9 ticket includes two timestamps indicating the elapsed time since the last user
10 authentication.

11 The authentication server also copies certain elements of the user's profile
12 information to the affiliate server (step 242). The affiliate server then generates a
13 personalized web page and communicates the web page to the user's browser (step
14 244). The affiliate server also copies a cookie to the client computer system
15 containing information indicating that the user of the client computer system has
16 been authenticated and indicating the period of time during which the
17 authentication is valid. Each time the user enters a new web page request on the
18 same affiliate server, the data in the cookie is copied to the affiliate server along
19 with the page request. Thus, the affiliate server will not repeatedly check the
20 authentication of a user during each subsequent page request.

21 In an embodiment of the invention, a particular affiliate server may utilize
22 only a portion of the services available from the authentication server. For
23 example, the affiliate server may perform its own authentication of the user, but
24 requests the user profile information from the authentication server. In another
25 example, the affiliate server may rely on the authentication server to authenticate

1 the user, but the affiliate server ignores the user profile information and, instead,
2 collects information from the user itself.

3 In one embodiment of the invention, the same login ID is used to identify a
4 particular user on all affiliate servers. However, this configuration presents a
5 situation in which affiliate servers could exchange information collected about the
6 user with other affiliate servers, relying on the common login ID. To avoid this
7 situation, a second embodiment of the invention uses a different login ID for each
8 of the affiliate servers. This use of different login IDs is transparent to the user,
9 who only knows of the login ID used to log into the authentication server. The
10 authorization server maintains a list or cross-reference table that correlates the
11 user's login ID on the different affiliate servers. In this embodiment, the affiliate
12 servers do not know the login ID used on other affiliate servers for the same user
13 and, therefore, cannot exchange information about the user with other affiliate
14 servers.

15 A particular embodiment of the invention has been described and illustrated
16 herein with reference to multiple web servers and an authentication server coupled
17 to a common data communication network. However, the teachings of the present
18 invention can be applied to any type of web server or other computing device that
19 accesses a centralized authentication system to authenticate a user and retrieve
20 associated user profile information. Furthermore, the present invention can be
21 utilized without requiring a data communication network. Instead, one or more
22 temporary or permanent data communication links are established between an
23 authentication server and an affiliate server for exchanging data.

24 Thus, a system has been described that allows a web server to authenticate
25 a user seeking access to the web server. The authentication is performed by an

1 authentication server without exposing the user's authentication information (e.g.,
2 password) to the web server. The web server receives an authentication ticket
3 from the authentication server indicating whether the authentication was
4 successful and further indicating the time since the last user authentication. The
5 authentication server may also provide user profile information to the web server
6 if the user is authenticated. Thus, the authentication server provides a centralized
7 device for authenticating users without exposing the user's confidential login
8 information to an affiliate server. This single user profile may be provided to
9 multiple affiliate servers without requiring repeated entry of information by the
10 user (i.e., entering user information at each new web site visited). Once the user
11 has been authenticated by the authentication server, the user can visit multiple web
12 sites that are affiliated with the authentication server without re-entering the
13 authentication information for each web site.

14 Although the invention has been described in language specific to structural
15 features and/or methodological steps, it is to be understood that the invention
16 defined in the appended claims is not necessarily limited to the specific features or
17 steps described. Rather, the specific features and steps are disclosed as preferred
18 forms of implementing the claimed invention.

19
20
21
22
23
24
25